The claims:

1) A method for the remote printing of a document by use of a network, the method including the steps of:
   (a) receiving at a server the document as sent from a sender;
   (b) the server forwarding the document to a recipient;
   (c) the document being authenticated prior to being forwarded to the recipient; and
   (d) the server receiving instructions from the sender regards printing controls and the server implementing those controls on the recipient.

2) A method for the remote printing a document by use of a network, the method including the steps of:
   (a) a sender sending the document to a server to enable the server to forward the document to a recipient;
   (b) the document being authenticated by the sender prior to sending it to the server; and
   (c) sending to the server instructions for controlling the printing of the document to enable the server to implement those controls on the recipient.

3) A method for printing of an authenticated document received remotely by use of a network, the method including the steps of:
   (a) a recipient receiving the authenticated document from a server, the server having received the authenticated document from a sender;
   (b) the server providing implementation of printing controls on the recipient, the server having received the printing controls from the sender.

4) A method as claimed in claim 1, wherein the printing controls include the ensuring that the document as printed has a content that is exactly the same as the document content as sent by the sender.

5) A method as claimed in claim 1, wherein the printing controls include anti-forgery controls.

6) A method as claimed in claim 1, wherein the printing controls include anti-copying controls.

7) A method as claimed in claim 1, wherein the printing controls include controls on a number of copies of the document that are to be printed.

8) A method as claimed in claim 1, wherein the recipient includes a printer, the server providing the printing controls to the printer for the printing of the document, and the server enables a secure document delivery from the sender through the server to the recipient.

9) A method as claimed in claim 8, wherein the server is a trusted agent to the sender in printing control, and is a trusted third party in document verification services.

10) A method as claimed in claim 9, wherein the server stores a hash of the document, and at least one content feature of the document, and uses them for document verification.

11) A method as claimed in claim 10, wherein secure document delivery and printing control is based on a trusted document structure including one or more from the group consisting of:

a) the document itself;
b) a hand signature;
c) a digital signature;
d) an optical watermark;
e) content features of the document;
f) usage control and audit trail;
g) a seal of the sender; and
h) an expiry date.

12) A method as claimed in claim 11, wherein the sender authorises the document.

13) A method as claimed in claim 1, wherein the method uses a public key infrastructure to provide nonrepudiation, privacy and security in the delivery of the document.

14) A method as claimed in claim 11, wherein the digital signature is applied to the document, the digital signature being that of one or more selected from the group consisting of: the sender, the server, the recipient.

15) A method as claimed in claim 1, wherein the sender is registered with the server before the sender can send the document, and the recipient is registered with the server before the recipient can receive the document.

16) A method as claimed in claim 11, wherein a document hash and the content features are sent with the document for validation, and a hash and content feature of the document are kept in the server for future verification.

17) A method as claimed in claim 1, wherein the method uses a secure document transfer channel provided by Secure Socket Layer protocol, and authentication of the sender and the recipient is by using user identity and at least one password.

18) A method as claimed in claim 1, wherein the method uses encryption techniques for secure document delivery, a key to decrypt the document being sent directly to the recipient by a carrier means selected from the group consisting of: email, telephone, mail, courier and personal delivery; and the document as printed is protected against unauthorised copying and forgery by using an authentication means selected from the group consisting of: optical watermark, special ink, special paper and special printing materials.

19) A method as claimed in claim 11, wherein the optical watermark has a counterfeit-proof layer, the printer being calibrated to achieve a high level of performance of the counterfeit-proof layer.

20) A method as claimed in claim 19, wherein the calibration is performed using a printing language without manual intervention, the printer being secure in the printing control process.

21) A method as claimed in claim 20, wherein the printer includes a secure memory, a secure central processing unit, and a secure clock, the secure memory being used to store a private key, the secure central processing unit being used to prevent run-time attacks; and the secure clock being used to keep time.

22) A method as claimed in claim 21, wherein the printer and the server system perform secure handshaking to authenticate each other, the printer and the server using one or more selected from the group consisting of a public key pair or the symmetry key of the printer.

23) A method as claimed in claim 11, wherein the server sends an encrypted form of the document hash, the optical watermark, and printing instructions, to the printer.

24) A method as claimed in claim 23, wherein the printer receives the document through client software, decrypts the document, and verifies the document with a hash and time stamp before printing, and adds the optical watermark during printing.

25) A method as claimed in claim 24, wherein the document is deleted from the secure memory immediately after printing, and an audit trail record is created in the server.

26) A method as claimed in claim 1, wherein there is included client software that is downloaded to a machine of the recipient for the printing of the document, the

recipient being trusted in the printing control process to minimise attack on the client software.

27) A method as claimed in claim 26, wherein the server communicates with the printer through the client software to verify a serial number of a printer of a machine of the recipient and an internet protocol address of the recipient, check the status of the printer, locks a control panel of the printer, sets all necessary printer settings, sends to the printer the document and instructions for printing the document, and reset the printer settings after the printing process is completed, and creates an audit trail record in the server.

28) A method as claimed in claim 11, wherein the seal includes one or more selected from the group consisting of: the hand signature and the seal; the seal including a common seal which is common to all printed copies, and a unique seal which is unique to each printed copy.

29) A method as claimed in claim 26, wherein the client software has a basic part and a sensitive part, the sensitive part being more susceptible to attack than the basic part; the basic part being sent to the recipient when the recipient is registered with the server; the sensitive part being downloaded to the recipient's machine for the printing of the document and is deleted from the recipient's machine upon the completion of the printing to protect the sensitive part from attack.

30) A method as claim in claim 29, wherein an encrypted form of the sensitive part is sent to the recipient when the recipient is registered with the server, the server managing the decryption key; the sensitive part being decrypted when and as required.

31) A method as claimed in claim 29, wherein a hash result of the basic part is taken at the same time as or before the basic part is sent to the recipient, the hash result being stored in the server; and when the recipient requires printing of the

document a second hash result of the basic part is taken and compared with the hash result before printing is authorized by the server.

32) A method as claimed in claim 27, wherein an execution time for the execution of components of the sensitive part is recorded in the server, and compared with the time taken for the execution of the components during the printing of the documents; the printing being terminated if the time taken is significantly longer than the execution time.

33) A method as claimed in claim 1, wherein the printing controls are implemented in response to the recipient requesting the printing of the document.

34) A method as claimed in claim 1, wherein the printing control is carried-out off-line, the server not participating in the printing process.

35) A method as claimed in claim 34, wherein there is provided a hardware device at the recipient to act on behalf of the server.

36) A method as claimed in claim 35, wherein the hardware device is for controlling the printing of the document, the hardware device including a secure memory, a delete-after-read memory, a central processing unit with an on-chip program, and an interface; the hardware device being registered with the server.

37) A method as claimed in claim 35, wherein the recipient includes a printer, the hardware device being integral with the printer; the printer being registered with the server.

38) A method as claimed in claim 36, wherein the secure memory has an accessible memory that can be accessed only when a password of a user is entered and verified, the access being only to a block of the accessible memory relevant for that user; and a controlled memory for internal use, the controlled memory being divided into a plurality of blocks, there being one controlled memory block for each user.

39) A method as claimed in claim 38, wherein the controlled memory is for the storage of secret keys, serial numbers, user's private keys and the recipient's ID key.

40) A method as claimed in claim 34, wherein the printing controls include the issuing of a license for the recipient to print the document, the license including a number of copies of the document authorized for printing.

41) A method as claimed in claim 40, wherein each license has a license key, the license key being used to encrypt the unique seal; the license keys being sent to the recipient by the server in an encrypted form and being installed in the hardware device.

42) A method as claimed in claim 41, wherein the server can add to the number of license keys, the server generating a new license key set and a new top-up key, the new license key set and the new top-up key being encrypted with the previous top-up key prior to being sent to the recipient by the server and being installed in the hardware device.

43) A method as claimed in claim 40, wherein each license includes an expiry date after which printing of the document using that license will no longer be possible.

44) A method as claimed in claim 42, wherein the new license key set is sent separately from the document.

45) A method as claimed in claim 42, wherein the new license key set is sent with the document.

46) A method as claimed in claim 40, wherein prior to the sender sending the document, the sender's common seal, a timestamp for sending, and the expiry date, are encrypted with a first session key to give an encrypted result, and the

encrypted result and the document are encrypted with a second session key to give a second encrypted result.

47) A method as claimed in claim 46, wherein a hash result is included in the second encrypted result to provide a means for checking data integrity.

48) A method as claimed in claim 40, wherein the print controls can be to view the document but not to print the document, a license not being required for viewing.

49) A method as claimed in claim 11, wherein the expiry date is checked before printing of the document is authorized and, if the expiry date has passed, printing of the document is not allowed.

50) A method as claimed in claim 1, wherein the sender and the server are the same, all functions of the sender being performed by the server.

51) A method as claimed in claim 50, wherein the sender is an authority which issues a secure hardware device to each of a plurality of recipients, the document and license keys being sent to each of the recipients by a network, each recipient using the secure hardware device to print the document, the document being sent by the recipient to a customer of the recipient as a printed or electronic document, the secure hardware device controlling the sending of electronic documents, the secure hardware device creating an audit trail and sending it to the authority whenever new license keys are topped-up.

52) A method as claimed in claim 51, wherein the document is selected from the group consisting of: postage stamps, tax invoice, tax receipt.

53) A method as claimed in claim 52, wherein a value of each postage stamp, tax invoice, and tax receipt is included in the audit trail.

54) A method as claimed in claim 53, wherein the authority determines tax payable based on the values included in the audit trail.

55) A method as claimed in claim 34, wherein there is provided a secure software program to implement the printing controls at the recipient.

56) A method as claimed in claim 55, wherein the software program is implemented in a distributed manner to assist in preventing software attacks.

57) A method as claimed in claim 56, wherein the secure memory for the licence keys and audit trails is implemented in a distributed manner.

58) A hardware device for use with a user's machine to enable control of printing of at least one document by the machine, the hardware device including a secure memory, a delete-after-read memory, a central processing unit with an on-chip program, and an interface.

59) A hardware device as claimed in claim 58, wherein the secure memory has an accessible memory that can be accessed only when a password of the user is entered and verified, the access being only to a block of the accessible memory relevant for the user; and a controlled memory divided into a plurality of blocks, there being one controlled memory block for each user.

60) A hardware device as claimed in claim 59, wherein the controlled memory is for the storage of secret keys, serial numbers, user's private keys, and the user's ID key.

61) A hardware device as claimed in claim 58, wherein the hardware device is implemented as a secure software program.

62) A hardware device as claimed in claim 61, wherein the software program is implemented in a distributed manner to assist in preventing software attacks.